

ABSTRACT

Content data encrypted with a content key, the content key encrypted with an individual key specific to an information sending device, and the individual key encrypted with a distribution key that is updated in a predetermined cycle, and supplied are sent to an information receiving device, and the information receiving device decrypts the individual key with the distribution key, decrypts the content key with the individual key, and decrypts the content data with the content key. Thus, the information sending device does not have the distribution key, and accordingly piracy of content data can be prevented with a simple configuration. Also, the information receiving device sends the content key and a playback command to other apparatuses. Thus, other apparatuses can play back contents using the playback command and the content key. Furthermore, the information sending device decrypts the content key with the distribution key before being updated, and stores the same. Thus, contents purchased by an advance order can be actually purchased regardless of expiration dates of the distribution key. Furthermore, usage right is passed from a first information receiving device to a second information receiving device different in registration information at the time of using contents. Thus, contents can be used among information receiving devices different from each other in registration information.